

There is provided a data processor wherein

There is provided a data processor wherein a plain text is encrypted to a cipher text by using an encryption key and/or a cipher text is decrypted to a plain text by using a decryption key, which device is constructed of a plurality of key conversion functions f_k sequentially connected, which each are an involution type, and which conduct key conversion processing and output extended keys based on the key for encryption or decryption, or key conversion results, a key conversion section in which the key conversion results are sequentially transferred between the key conversion functions in the order or the reverse order, a plurality of round functions f_r sequentially connected, which are an involution type, and which conducts encryption and/or decryption by using extended keys, and a data randomize section in which processing results in the round functions f_r are sequentially transferred between the round functions f_r in the order or the reverse order. With the device, the scale of a secret key encryption device can be small, security can be increased and further, key management can be conducted with ease.